PCMAV, Antivirus Made in Indonesia

Berangkat dari keprihatinan terhadap serangan virus yang semakin mengganas dan susahnya menemukan antivirus yang mampu mengatasi virus lokal secara tuntas dan akurat, maka kami ciptakan PC Media Antivirus (PCMAV) untuk Anda. Jaminan kepuasan 100% dari pembaca *PC Media* merupakan tujuan utama kami.

Anton R. Pardede

Seorang pembaca *PC Media* sempat menanyakan mengapa dalam melakukan pemeriksaan virus di CD-nya, *PC Media* mempercayakannya hanya kepada NOD32? Bukankah McAfee VirusScan maupun Norton Antivirus lebih terkenal dan telah digunakan oleh media komputer lainnya di Indonesia? Jawabannya simpel tapi *dalem*: saya sebagai pemimpin redaksi majalah ini merupakan pemerhati antivirus di Indonesia. *Ngerti donk* maksudnya?

Penggunaan NOD32 merupakan pilihan berdasarkan pengalaman profesional saya berkecimpung di dunia virus komputer dan keamanan data selama kurang lebih 13 tahun lamanya. Bukan berarti antivirus yang lain kurang baik, ini masalah rasa dan kecocokan fungsi dalam penggunaanya. Walau begitu, saya justru tidak menyarankan NOD32 ini digunakan oleh orang awam dalam penggunaan sehari-hari. Tetapi perlu diingat bahwa NOD32 ini hanya kami gunakan untuk memeriksa secara mendalam file-file yang akan kami taruh di CD. Bagaimana soal pembersihan sistem yang telah dijangkiti virus, terutama virus lokal? Inilah titik kelemahan antivirus luar negeri, termasuk NOD32 sekalipun.

Mengenal Saja Tidak Cukup

Semakin hari ternyata penyebaran virus komputer semakin luar biasa saja. Mulai dari orang awam sampai perusahaan multinasional sekalipun tak luput dari serangan virus komputer. Ini di luar prediksi saya sebelumnya yang mengira tingkat keamanan Windows XP sudah cukup untuk menghambat penyebaran virus. Jaman berubah. Membuat virus komputer kini dapat dengan mudah dilakukan, bahkan dengan Visual Basic sekalipun. Internet dan USB Flash Disk merupakan media utama penyebaran virus-virus saat ini, terutama di Indonesia. Tetapi, faktor utama tetap pada kelalaian manusianya (atau kecerdasan si pembuatnya ya?).

Akhir tahun 2005 kemarin merupakan puncak penyebaran virus di Indonesia yang dimotori oleh virus Brontok (karena keterbatasan halaman, hasil analisis Brontok yang sebenarnya dapat Anda baca di edisi depan). Berbagai e-mail yang masuk ke saya menanyakan soal pembasmian virus ini. Dan soal pembasmian virus, terus terang saya pun bingung merekomendasikan anti-

virus yang cocok. Di sinilah *feeling* saya mengatakan bahwa sudah saatnya *PC Media* membuat antivirus yang bukan sekadar hanya mampu mengenali virus, tetapi mampu pula mengatasinya secara tuntas dan akurat, baik di file, folder, memori, registry, maupun objek lainnya yang berhasil dimanfaatkan oleh virus. Selain itu, sifatnya pun harus *portable* agar mudah digunakan tanpa instalasi dan dapat dijalankan di USB Flash Disk sekalipun.

Dengan tim kecil yang dibentuk hanya dalam waktu sebulan; seorang arsitek dan seorang *developer* antivirus serta diperkuat seorang analis virus yang berpengalaman, maka lahirlah **PC Media Antivirus** *(*PCMAV*)*, antivirus satu-satunya di dunia yang mampu mengatasi virus Brontok secara tuntas dan akurat 100%. Segera menyusul untuk virus-virus lainnya yang menyebar di Indonesia di *PC Media* edisi berikutnya.

Pertama dan Satu-satunya

Ya, pernyataan tersebut tidak mengada-ngada serta ditunjang dengan fakta dan penelitian. Dalam hal penanganan virus komputer, ketegasan terkadang diperlukan untuk meyakinkan pengguna awam yang terlanjur mendapatkan informasi kurang akurat dari pihak yang pengalamannya patut dipertanyakan.

Kami telah melakukan tes komprehensif terhadap *update* terbaru antivirus komersial yang ada saat ini, termasuk beberapa yang memiliki distributor/*reseller* di Indonesia, dan hasilnya tidak ada satu pun dari antivirus tersebut yang mampu mengatasi Brontok secara tuntas.

Mulai dari tersisanya beberapa file virus di harddisk, situs yang masih terblok, pesan *registry error, Folder Option* yang masih menghilang, sampai Brontok bisa aktif kembali merupakan contoh yang akan didapat hasil penggunaan antivirus komersial yang ada di pasaran.

PCMAV berbeda. Dengan teknologi khusus pembasmian virus yang kami kembangkan sendiri dan tanpa proses instalasi, PCMAV mampu mengatasi Brontok dan variannya secara akurat dan tuntas baik di memory, registry, file dan folder yang tersembunyi, bahkan di *Scheduled Tasks* sekalipun. Tidak peduli sekalipun Brontok mengganti file dan *key*-nya secara acak (di varian Brontok terbaru), PCMAV tetap mampu memburu dan membasminya tanpa ampun.

Teknologi yang Digunakan

Untuk menambah keandalannya, selain menggunakan *engine*-nya sendiri, PCMAV juga memanfaatkan *core engine* dan *database* dari ClamAV (antivirus *open-source* untuk Unix, *www.clamav.net*). Kombinasi keduanya sungguh dahsyat. Saat ini, PCMAV mampu mengenali lebih dari 40.000 virus yang ada dan tentunya akan terus bertambah.

Selain itu, kami juga mengembangkan pendeteksian heuristik yang unik agar PCMAV mampu pula mengenali varian Brontok lainnya yang belum sempat diidentifikasi untuk saat ini.

Penggunaannya Mudah

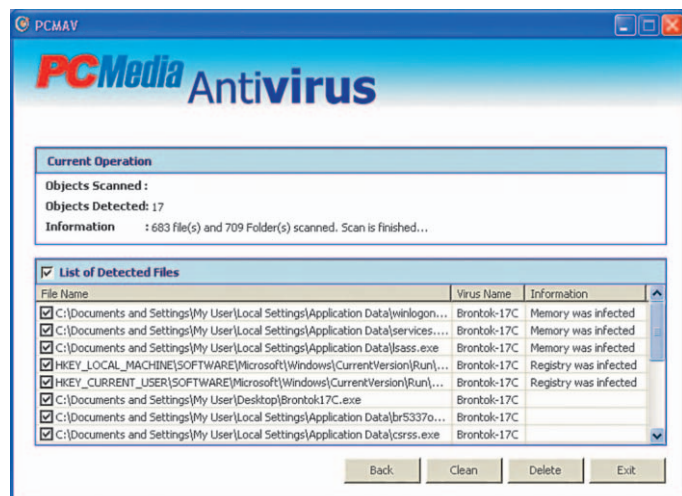
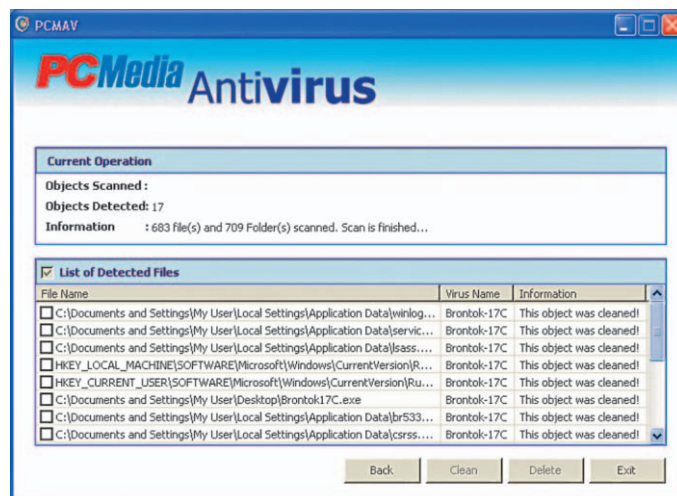
PCMAV ini dirancang sedemikian rupa agar mudah dijalankan, bahkan oleh orang awam sekalipun. Jalankan PCMAV.EXE yang ada di CD Emergency Pack edisi ini, pilih drive yang Anda ingin periksa, lalu tekanlah tombol *Scan*.

Pertama-tama PCMAV akan memeriksa memory, lalu registry sebelum memeriksa file yang ada di drive tujuan. Jika virus yang ada di database internal PCMAV terdeteksi (untuk saat ini adalah Brontok sebanyak 16 varian), maka Anda tinggal mencentang (✓) "List of Detected Files" agar seluruh file yang terdeteksi terseleksi. Bagi Anda pengguna mahir, dapat memilih secara individu satu per satu file dengan mencentang (✓) di depan file yang terdeteksi. Setelah itu, tekanlah tombol "Clean" untuk mulai membasminya secara tuntas.

Lain halnya jika virus yang terdeteksi dikenali oleh engine ClamAV, maka hanya ada pilihan tombol "Delete" saja untuk menghapus objek yang terdeteksi.

Pengembangan

Walau telah diuji berkali-kali, tentu saja PCMAV tidak akan luput dari *bug (*kekeliruan minor pemrograman*)* yang mungkin timbul. Untuk itu, sudilah kiranya melaporkan kepada kami jika Anda menemukan kesalahan dalam pemakaian PCMAV sehari-hari.

Kami akan selalu mengimprovisasi PCMAV agar Anda terpuaskan dan nyaman dalam menggunakannya.

Virus Brontok terdeteksi.

Virus Brontok dimusnahkan.

FAQ: PC Media Antivirus 1.0 RC1

Berikut ini merupakan rangkuman beberapa pertanyaan yang sering diajukan selama dilakukan beta tes terhadap PC Media Antivirus 1.0 (PCMAV).

Anton R. Pardede dan Arief Prabowo

Mengapa PC Media Antivirus?
Mengapa tidak? :)

Apakah di setiap edisi terbaru PC Media selalu tersedia PCMAV?
Ya, PCMAV mulai tersedia di *PC Media* edisi 03/2006 ini.

Di mana bisa mendapatkan update terbaru PCMAV?
Saat ini, PCMAV terbaru bisa didapatkan secara eksklusif hanya di CD *PC Media* edisi terbaru, baik di edisi regular maupun edisi ekonomis.

Apakah PCMAV hadir untuk menggantikan antivirus komersial yang telah ada di pasaran?
Tidak. PCMAV hadir untuk saling melengkapi antivirus yang sudah ada di pasaran.

Mengapa tampilan PCMAV tidak menggunakan bahasa Indonesia?
Pengembangan PCMAV dimaksudkan untuk multibahasa. Basis *default*-nya adalah bahasa Inggris agar lebih nyaman dikembangkan ke bahasa Indonesia dan bahasa asing lainnya, bahkan ke bahasa daerah sekalipun bisa dilakukan.

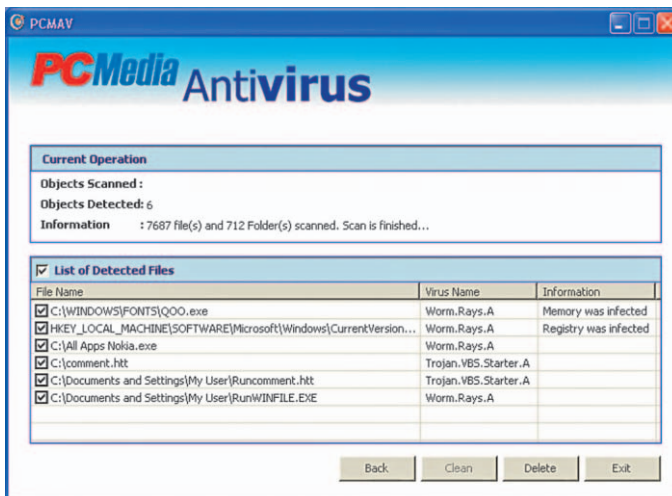
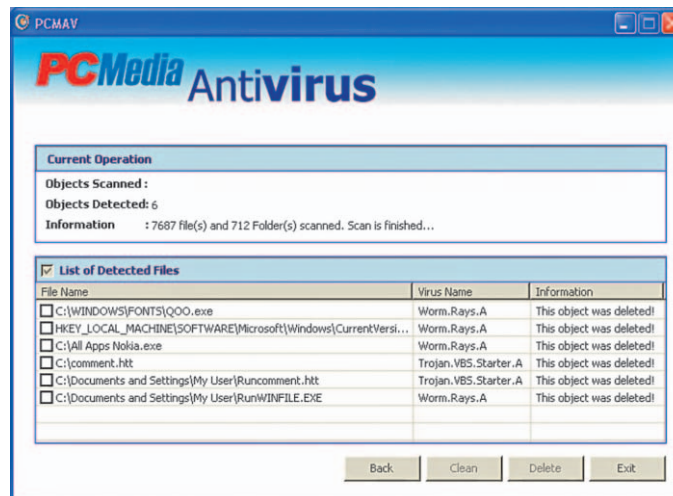
Mengapa tampilan PCMAV tidak mengikuti tren tampilan Windows XP?
Di versi RC1 dibuat hanya dalam waktu sebulan lamanya. Mohon maklum kiranya apabila dirasa tampilan PCMAV masih terasa "kuno". Di *final release* nanti tampilan PCMAV akan lebih trendi dan lebih fungsional *kok*.

Apa arti RC1 di belakang versi PCMAV?
RC1 singkatan dari *Release Candidate 1*. Istilah lainnya, meminjam istilah pembukaan mal/plaza, RC itu *soft opening* sebelum *grand opening* (*Final Release*). Tentu segala masukan dari Anda akan kami jadikan untuk membuat PCMAV ini semakin baik.

Di operating system mana saja PCMAV bisa beroperasi?
Saat ini, kami telah mengujicobanya dan berjalan baik di Windows XP Home dan Windows XP Professional.

Apakah PCMAV ini *freeware*?
Ya. PCMAV ini bersifat *freeware*.

Apakah ada rencana menjadikan PCMAV menjadi software komersial?
Saat ini belum ada, tetapi tidak tertutup kemungkinan kami kembangkan versi lain yang bersifat profesional untuk kepentingan komersial. Tentu saja versi ini akan ditunjang fitur tambahan, seperti *real-time protection* baik untuk file, registry, maupun e-mail; *online update*, dokumentasi yang lengkap, serta dukungan teknis. Apa ada yang tertarik memesannya? :)

Mengapa PCMAV begitu percaya diri mengatakan mampu mengatasi virus yang menyebar di Indonesia secara tuntas dan akurat 100%?
Boleh dibilang saat ini kamilah satu-satunya di Indonesia yang terpercaya memiliki pengalaman dan *knowledge* khusus di bidang antivirus lebih dari 13 tahun lamanya. Selain aktif sebagai narasumber di media elektronik dan cetak nasional, kami juga dipercaya mengisi berbagai seminar antivirus di Indonesia. Berbagai program antivirus telah kami hasilkan, termasuk antivirus

Virus lain (versi ClamAV) terdeteksi.

Virus lain (versi ClamAV) telah dihapus.

CIH (SVCIH) yang cukup fenomenal di medio 1998-1999. Dengan pengalaman tersebut, berbagai kelemahan dan kelebihan antivirus yang ada di pasaran kami amati dan pelajari, terutama soal keakuratan dan ketuntasannya dalam mengatasi virus lokal. Dan lagi jika PCMAV tidak punya kelebihan seperti itu, buat apa repot-repot kami membuatnya untuk Anda?

Brontok itu sebenarnya virus atau worm?
Secara teknis merupakan *worm*. Tetapi, kami lebih sepakat menggunakan istilah virus untuk worm mengingat sifatnya yang mampu menyebar dengan menggandakan dirinya sendiri meski tanpa menginfeksi file.

Apakah PCMAV mampu mengatasi Brontok dalam modus normal tanpa perlu ke safe mode?
Dari hasil uji coba kami di Windows XP Professional, PCMAV mampu mengatasi Brontok dalam modus normal sekalipun. Sebagai catatan, antivirus lain tidak mampu melakukannya dalam modus normal.

Apakah hanya Brontok yang dapat dibasmi secara tuntas?
PCMAV 1.0 RC1 yang terbit di edisi 03/2006 hanya mengenal 16 varian Brontok yang mampu dibasmi secara menyeluruh. Walau begitu, saat ini di lab antivirus kami telah mengantri sejumlah virus lain yang banyak menyebar di Indonesia untuk dianalisis dan dibuatkan modul pembasminya.

Mengapa antivirus luar negeri yang digembar-gemborkan mampu mengatasi Brontok oleh distributor/reseller-nya di Indonesia ternyata tidak mampu membasminya secara tuntas, malah membuat Windows error?
Entahlah, kami sendiri tidak mau berspekulasi akan hal tersebut. Silakan tanyakan langsung ke distributor/*reseller*-nya di Indonesia.

PC saya terinfeksi virus, apakah PC Media bisa membuatkan pembasminya?
Dengan senang hati. Kirim saja file yang dicurigai terinfeksi virus kepada kami melalui e-mail, sebaiknya di-ZIP dan diberi *password*.

Keberatan tidak jika saya kirimi virus buatan saya?
Tentu saja kami tidak keberatan. :)

Apakah benar tim PCMAV menganalisis sendiri virus tersebut?
Tim analisis virus kami terdiri dari profesional pilihan di bidangnya. Untuk membuat modul pembersihnya, kami membedah secara mendalam satu per satu virus tersebut. Hasilnya, pendeteksian dan pembasmian virus tersebut dapat dilakukan secara tuntas dan akurat 100% di seluruh objek yang terjangkiti virus tersebut. Jika dirasa menarik, hasil analisis tersebut akan ditampilkan di rubrik antivirus pada *PC Media* edisi terbaru.

Mengapa hasil analisis distributor antivirus luar negeri di media lokal terkadang bertolak belakang dengan hasil analisis tim PCMAV?
Kami duga itu merupakan hasil analisis tim antivirus luar negeri yang diartikan dengan kurang baik oleh pihak distributornya. Atau karena bukan bidangnya bisa jadi mereka hanya menduga-duga saja akibat kekurangpahaman yang mendalam terhadap virus itu sendiri. Kami tidak mau berspekulasi soal ini, menganalisis virus komputer merupakan pekerjaan yang cukup kompleks, serta memerlukan pengetahuan, pengalaman dan seni tersendiri.

Mengapa pemeriksaan PCMAV agak lambat di komputer saya?
Bisa jadi spek komputer yang kurang memadai atau sedang memeriksa file yang terkompresi (.ZIP). Jika Anda kurang nyaman akan hal ini, silakan matikan centangan (✓) di pilihan "Scan for archive", walau tidak kami sarankan untuk mendapatkan hasil pemeriksaan yang optimal.

Bagaimana menggunakan PCMAV secara optimal?
Kami telah mengaktifkan secara *default* semua opsi pemeriksaan file untuk mendapatkan hasil yang optimal. Kami menyarankan untuk tidak mematikan opsi *default* ini. Selain itu, matikan fasilitas "System Restore" di Windows XP Anda. Ketika komputer Anda yang terinfeksi telah selesai diatasi, sebaiknya ulangi pemeriksaan sampai virus benar-benar tidak ditemukan. Setelah itu, *booting* komputer Anda lalu lakukan pemeriksaan ulang sekali lagi. Tentu saja ada "harga" yang harus dibayar berupa waktu yang cukup lama untuk memeriksa secara optimal seluruh file yang ada di komputer Anda.

Apakah heuristik itu?
Teknik heuristik merupakan metode yang mampu mengenali virus baru yang belum dikenal oleh sebuah antivirus. Di *PC Media,* kami terus melakukan pengembangan teknik heuristik terbaru agar mampu "mengajari" PCMAV untuk mengenali virus-virus baru dengan lebih akurat, bahkan yang bersembunyi di dalam *registry* sekalipun.

Mengapa perlu menggunakan engine ClamAV?
Tentu saja untuk memperkuat kemampuan PCMAV agar bisa lebih banyak mengenali virus lainnya, selain virus-virus lokal yang menyebar di Indonesia. Selain itu, saat ini kami sedang mengembangkan modul dan database khusus agar kompatibel dengan format database virus dari ClamAV dan Open AntiVirus sehingga akan saling melengkapi.

Apakah engine ClamAV tidak akan saling tumpang tindih dalam mengidentifikasi virus dengan engine internal PCMAV?
Tidak. ClamAV digunakan di lapis (*layer*) atas, sedangkan PCMAV di lapis bawah. Apapun hasil dari lapis atas secara otomatis akan tersaring oleh hasil lapis bawah. Dengan kata lain, kendali utama tetap dipegang oleh *engine* internal PCMAV.

Apakah PCMAV mampu mengatasi spyware?
Saat ini belum. Tetapi, kami ada rencana ke arah sana. Saat ini, *engine* khusus untuk mengatasi spyware sedang dalam pengembangan tahap awal. ■